What Is Claimed Is:

Sub a1

1. An enciphering apparatus, comprising:

enciphering means for enciphering data using a cryptographic key;

first generating means for generating a first key;

second generating means for generating a second key which is changed at a predetermined timing while the data is enciphered; and

producing means for producing the cryptographic key using the first key and the second key.

2. An enciphering apparatus according to claim 1, wherein said producing means produces a homomorphic cryptographic key.

Sub a2

3. An enciphering apparatus according to claim 1, wherein said producing means produces a cryptographic key with which a correct decipherment result is obtained even if the first cryptographic key and the second cryptographic key which compose the cryptographic key are used individually to successively decipher the enciphered data.

4. An enciphering apparatus according to claim 1, wherein said producing means adds the second key to a value whose initial value is the first key to produce the cryptographic key.

5. An enciphering apparatus according to claim 4,

wherein the first key has a number of bits larger than that of the second key, and said producing means adds the second key to bits at predetermined positions of the first key, extracts a bit at a predetermined position of a result of the addition and further adds the extracted bit to produce the cryptographic key.

6. An enciphering apparatus according to claim 5, wherein said producing means further updates the predetermined bits of the result of the addition with a result of the further addition of the extracted bit.

7. An enciphering apparatus according to claim 6, wherein said producing means selects predetermined bits from a result of the further addition of the extracted bits further at a predetermined timing to produce the cryptographic key.

8. An enciphering apparatus according to claim 1, further comprising transmission means for transmitting the data enciphered with the cryptographic key to another apparatus via a bus.

Sub a3 >

9. An enciphering method, comprising the steps of:

enciphering data using a cryptographic key;

generating a first key;

generating a second key which is changed at a predetermined timing while the data are enciphered; and

producing the cryptographic key using the first key and the second key.

10. A deciphering apparatus, comprising:

receiving means for receiving enciphered data;

deciphering means for deciphering the received data using a cryptographic key;

first generating means for generating a first key;

second generating means for generating a second key which is changed at a predetermined timing while the data is deciphered; and

producing means for producing the cryptographic key using the first key and the second key.

11. A deciphering apparatus according to claim 10, wherein said producing means includes first producing means for producing a first cryptographic key using one of the first key and the second key, and second producing means for producing a second cryptographic key using the other of the first key and the second key, and said deciphering means includes first deciphering means for deciphering the enciphered data using the first cryptographic key, and second deciphering means for deciphering the data deciphered by said first deciphering means further using the second cryptographic key.

12. A deciphering apparatus according to claim 11,

wherein said second deciphering means is formed from application software for processing the deciphered data.

Sub a4

13. A deciphering method, comprising the steps of:

receiving enciphered data;

deciphering the received data using a cryptographic key;

generating a first key;

generating a second key which is changed at a predetermined timing while the data is deciphered; and

producing the cryptographic key using the first key and the second key.

14. An information processing system, comprising:

a plurality information processing apparatus connected to each other by a bus;

said information processing apparatus including first information processing apparatus each having a function whose change is not open to a user, and second information processing apparatus each having a function whose change is open to a user;

each of said first information processing apparatus including:

first receiving means for receiving enciphered data;

first deciphering means for deciphering the data

received by said first receiving means using a cryptographic key;

first generating means for generating a first key;

second generating means for generating a second key which is changed at a predetermined timing while the data is deciphered; and

first producing means for producing the cryptographic key using the first key generated by said first generating means and the second key generated by said second generating means;

each of said second information processing apparatus including:

second receiving means for receiving enciphered data;

third generating means for generating the first key;

fourth generating means for generating the second key which is changed at a predetermined timing while the data is deciphered;

second producing means for producing a first cryptographic key using one of the first key generated by said third generating means and the second key generated by said fourth generating means;

third producing means for producing a second

cryptographic key using the other of the first key generated by said third generating means and the second key generated by said fourth means;

second deciphering means for deciphering the enciphered data received by said receiving means using the first cryptographic key; and

third deciphering means for further deciphering the data deciphered by said second deciphering means using the second cryptographic key.

15. An information processing method for an information processing system composed of a plurality information processing apparatus connected to each other by a bus, said information processing apparatus including first information processing apparatus each having a function whose change is not open to a user, and second information processing apparatus each having a function whose change is open to a user, comprising the steps performed by each of said first information processing apparatus of:

receiving enciphered data;

deciphering the data received in the receiving step using a cryptographic key;

generating a first key;

generating a second key which is changed at a

predetermined timing while the data is deciphered; and

producing the cryptographic key using the first key generated in the first generating step and the second key generated in the second generating step; and

the steps performed by each of said second information processing apparatus of:

receiving enciphered data;

generating the first key;

generating the second key which is changed at a predetermined timing while the data is deciphered;

producing a first cryptographic key using one of the first key and the second key;

producing a second cryptographic key using the other of the first key and the second key;

deciphering the enciphered data received in the receiving step using the first cryptographic key; and

deciphering the deciphered data further using the second cryptographic key.

Sub a5

16. An information processing apparatus, comprising:

receiving means for receiving data transmitted thereto through a bus;

producing means composed of a software program for producing a first cryptographic key and a second

cryptographic key which is changed at a predetermined timing while the data is deciphered from the data received by said receiving means;

first deciphering means for deciphering the enciphered data received by said receiving means using one of the first cryptographic key and the second cryptographic key produced by said producing means; and

second deciphering means for deciphering and processing the data deciphered by said first deciphering means further using the other of the first cryptographic key and the second cryptographic key produced by said producing means.

17. An information processing method, comprising the steps of:

receiving data transmitted thereto through a bus;

producing, from the received data, a first cryptographic key and a second cryptographic key which is changed at a predetermined timing while the data is deciphered;

deciphering the received enciphered data using one of the first cryptographic key and the second cryptographic key; and

deciphering the deciphered data further using the other of the first cryptographic key and the second

cryptographic key.

Add a6